



# SECURITY DOMAIN MINUTES

Date: December 19, 2002

## Attendees

- |  |  |
|--|--|
| <input type="checkbox"/> Steve Adams         | <input type="checkbox"/> Barb Kiso     |
| <input type="checkbox"/> Dustin Bieghler     | <input type="checkbox"/> Doug Less     |
| <input type="checkbox"/> Dawna Cape          | <input type="checkbox"/> Bob Meinhardt |
| <input type="checkbox"/> Curt Christian      | <input type="checkbox"/> Lora Mellies  |
| <input type="checkbox"/> Stephen Derendinger | <input type="checkbox"/> Gail Morris   |
| <input type="checkbox"/> Hank Henderson      | <input type="checkbox"/> Pete Wieberg  |

## New Business

- ☐ Attachments should not be sent in .DOT format because some agency firewalls block them.

## Old Business

- ☐ Reviewed December 5 Minutes  
*Minutes reviewed and accepted with no changes.*

- ☐ INFOCON Compliance Component

- ☐ Add "Domain" to the Associated Architecture Levels

- ☐ INFOCON removed from Definition text.

- ☐ Description: Beginning of paragraph altered to "Actions to uniformly heighten..." and final sentence changed to "This is a comprehensive..."
    - ☐ Rationale: Statement changed to "Incidents impact all personnel who use State of Missouri information systems. Awareness, assessment, and countermeasures protect systems while supporting mission accomplishment, and coordinate the overall effort through adherence to guidelines."

- ❑ Benefits: Text changed to “The State gains standard processes for assessing threats to the information infrastructure, and prescribes predictable responsive actions. When implemented consistently, each member of the State’s enterprise will have reasonable assurance that other members of the network present no greater vulnerability than the defined baseline standards. Provides an opportunity for the technology community to make senior management aware there is a constant battle to maintain network security, and that the entire State government is moving proactively to improve network assurance.”
- ❑ Discipline Name: Change “Operating” to “Operational”
- ❑ Government Body: Add the OIT web site.
- ❑ Keywords: Utilize same keywords used for technology area with the addition of countermeasures, alert, risk, and threat.

#### Cross-Domain Communications Procedure (Meinhardt)

- This matter was tabled for future discussion. Topic is non-critical since only one domain is active.

## Architecture Blueprint Products

#### Blueprint Packet Approval

- Approval process highlighted – Domain committee will send packets to the Architecture Review Committee (ARC). The ARC will review and submit feedback and/or approval/rejection.
- Group approved the following Blueprint Items (with changes listed in minutes) for submission to the ARC.
  - ❑ Security Domain
  - ❑ Management Controls Discipline
  - ❑ Operational Controls Discipline
  - ❑ Technical Controls Discipline
  - ❑ Incident Response Technology Area
  - ❑ Incident Response Reporting Compliance
  - ❑ Incident Awareness, Assessment, and Countermeasures Compliance

## Security Domain

### Security Domain text changes

- ❑ Benefits: Changed text to “Achieving confidentiality, data integrity, availability, and asset protection.”
- ❑ Boundary Limit Statement: Changed text to “Information access control, authorization, authentication, physical security as it relates to Information Technology. Protection, assurance, access management, auditing. Security is not synonymous with privacy.”
- ❑ Boundary Topics: As identified as “Topic Areas” within NIST – Risk Management; Review of Security Controls; Life Cycle; Authorize Processing (Certification and Accreditation); System Security Plan; Personnel Security; Physical Security; Production, Input/Output Controls; Contingency Planning; Hardware and Systems Software Maintenance; Data Integrity; Documentation; Security Awareness, Training, and Education; Incident Response Capability; Identification and Authentication; Logical Access Controls; Audit Trails
- ❑ Associated Disciplines: Management Controls; Operational Controls; Technical Controls

## Security Disciplines

### Management Controls

- ❑ Definition: Changed to include “and provides implementation authority”
- ❑ Boundary Topics: Personnel Security was added to the list (moved from NIST’s Operation classification). Some confusion arose concerning the Technology Area list versus Boundary Topics. The group discussed usage of Boundary Topics (previously Subject Areas), the rationale for their existence and what they mean. These items were used to lay the groundwork of topics the ATC felt the domain committee should cover. They may or may not become Technology Areas.

### Operational Controls

- ❑ Rationale: Changed to “Provides consistent controls for Administrators to secure the enterprise.”
- ❑ Benefits: Qualified “behavior” as “consistent behavior.” Replaced “individual responsibilities” with “defines responsibilities.”





### Technical Controls

- ❑ Benefits: Replaced “efficiency” and last item with “automation”





## Incident Response Technology Area

-  “Domain” was added to the Associated Architecture Levels section.

### Incident Response Technology Area


-  Template Change: Move Keywords below technology area detail and change associations to mirror other templates Associated Architecture Levels section.
-  Benefits: Changed to “Consistent method of evaluation and associate metrics; decrease spread; minimize damage; fulfills risk mitigation; limits impacts; promotes awareness; proactively improves network assurance; increases communication”
-  Keywords: Changed to include the items from the keywords on the two incident response compliance templates.
-  The question was raised concerning what happens if you have more than one standard organization or government body. In those cases, the rows would be repeated. However, this section deals with the main body(ies) that define the area, not necessarily all organizations that could be linked.

### Incident Response Reporting Compliance

-  Rationale: Changed to “Minimizes the damage from security incidents and facilitates communication throughout State agencies.”
-  Discipline Name: Changed from “Operating” to “Operational”
-  Standard Organization: Removed Gail Wekenborg’s name – individuals’ names should not be used in any Blueprint document due to potential for personnel changes.
-  Key Words: INFOCON; incident response; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; communication; denial of service

## Technology Areas

## Technology Area Definitions

-  Definition listing is a working document for the committee – to serve as a reference for current and future discussion and documentation.

■ Definitions approved with the following changes:

- ❑ Entity Authentication: Replace “Entity Authentication” with “Authentication”. Technology Area should include both User and Entity Authentication. Eliminate “most often” in the usage example. Biometrics, tokens, and cookies were added to the key word listing.
- ❑ Intrusion Detection System: Replaced “network” with “network / host”
- ❑ Information Classification: Expand classification statement to include integrity, availability, and confidentiality.

## Technology Scan Reviews

### ■ Virus Detection and Elimination

- Bob receive group approval to his request for the Domain to document their Virus recommendations and submit them to ITAB. The issues had already been broached within ITAB and this would give the group the opportunity to drive the resolution.
- Dustin discussed Novell virus software products within the Secretary of State’s Office, while Hank added information regarding McAfee products. Lora brought up Computer Associates and both she and Pete added information regarding Antigen.
- The group provided a steady flow of valuable information. Concern was expressed that the information would be lost because the technology scan worksheet wasn’t a Blueprint document. It was determined that the template could be eliminated and information entered directly on both the Product and Compliance templates. Following were the primary topics of discussion:
  - ❑ Will software be used on server, desktop, e-mail gateway, etc.?
  - ❑ Can it block attachments so that resources aren’t wasted on things such as .PIF files – known virus source.
  - ❑ Most products are per seat licensing. In the past, some contracts have allowed for copies to be taken to home PC’s (to prevent viruses from being carried into work from someone’s home computer).
  - ❑ Are .DAT files supported only when version is current? Hank mentioned that their agreement allowed for the State to be behind 3 releases, but must be on current version.
  - ❑ Different products should be used at different points (e.g. gateway vs. desktop) so that each point doesn’t have the same vulnerability.

- ❑ Method of updates – DoD uses Live Update, Pete mentioned Norton's Push updates, and Hank mentioned that all updates must be tested by Admin prior to distribution (users can't update).
- ❑ Extended protection of content filtering.
- ❑ Updates, upgrades, system checks, write permission, hot fixes

#### ■ The top products identified:

- ❑ Symantec (Novell)
- ❑ McAfee
- ❑ Trend
- ❑ Computer Associates (Inoculate)
- ❑ Sybari (Antigen)

#### ■ Homework

- ❑ Capturing primary product information for Product Components
  - Dustin – Novell
  - Hank – McAfee
  - Lora – Inoculate
  - Pete – Antigen
  - Gail – will canvass other agencies for other potential products
- ❑ Each member was encouraged to capture their own information in the form of best practices (for compliance) and product pros/cons.
  - Product Component – why one chosen over another
  - Compliance Component – best practices, configuration notes
- ❑ Group needs to look at all platforms.

#### ■ Additional Resources

- ❑ Tech Republic
- ❑ SANS
- ❑ <http://nsa.gov>
- ❑ NIST 800-5 and 500-1166
- ❑ ISO 17.799
- ❑ <http://www.trusecure.com>
- ❑ New Hampshire

#### ■ Password Policy Controls

##### ■ Technology Scan submitted by Curt for Mo-Guard information.

##### ■ Due to time constraints and clarification of homework, this item was not discussed. Committee members should look within agency, and at other sources, to complete Compliance templates regarding this area.

## Action Items



### Domain Committee



#### Virus Detection and Elimination

- ☐ Product template for products utilized within agency. **January 9, 2003**
- ☐ Compliance templates for best practices and/or configuration notes.

**January 9, 2003**



Password Policy Controls Compliance template **January 9, 2003**



### Facilitator / Scribe



Submit packet of Blueprint items to the Architecture Review Committee.  
**December 31, 2002**